1 <!-->

Google and Alphabet Vulnerability Reward Program (VRP) Rules

We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned and Alphabet (Bet) subsidiary web properties, running continuously since November 2010.

Services in scope

domains:

- *.google.com
- *.youtube.com
- *.blogger.com
- *.verily.com
- *.onduo.com
- *.projectbaseline.com

Bugs in Google Cloud Platform, Google- and Verily Life Sciences-developed apps, and extensions (published in Google Play, in the Apple App Store, or in the Chrome Web Store), as well as some of our hardware devices (Home, OnHub, Verily Life Sciences, and Nest) will also qualify. See our Android Rewards and Chrome Rewards for other services and devices that are also in scope.

On the flip side, the program has two important exclusions to keep in mind:

- **Third-party websites.** Some Google-branded services hosted in less common domains may be operated by our vendors or partners. We can't authorize you to test these systems on behalf of their owners and will not reward such reports. Please read the fine print on the page and examine domain and IP WHOIS records to confirm. If in doubt, talk to us first!
- **Recent acquisitions.** To allow time for internal review and remediation, newly acquired companies are subject to a six-month blackout period. Bugs reported sooner than that will typically not qualify for a reward.

Qualifying vulnerabilities

Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. Common examples include:

- Cross-site scripting,
- Cross-site request forgery,
- Mixed-content scripts,

New! In addition, significant abuse-related methodologies are also in scope for this program, if the reported attack scenario displays a design or implementation issue in a Google product that could lead to significant harm.

An example of an abuse-related methodology would be a technique by which an attacker is able to manipulate the rating score of a listing on Google Maps by submitting a sufficiently large volume of fake reviews that go undetected by our abuse systems. However, reporting a specific business with likely fake ratings would not qualify.

Note that the scope of the program is limited to technical vulnerabilities in Google-owned browser extensions, mobile, and web applications; please do not try to sneak into Google offices, attempt phishing attacks against our employees, and so on.

Out of concern for the availability of our services to all users, please do not attempt to carry out DoS attacks, leverage black hat SEO techniques, spam people, or do other similarly questionable things. We also discourage the use of any vulnerability testing tools that automatically generate very significant volumes of traffic.

Non-qualifying vulnerabilities

New! Visit our Bug Hunter University page dedicated to common non-qualifying findings and vulnerabilities.

Depending on their impact, some of the reported issues may not qualify. Although we review them on a case-by-case basis, here are some of the common low-risk issues that typically do not earn a monetary reward:

- **Vulnerabilities in *.bc.googleusercontent.com or *.appspot.com.** These domains are used to host applications that belong to Google Cloud customers. The Vulnerability Reward Program does not authorize the testing of Google Cloud customer applications. Google Cloud customers can authorize the penetration testing of their own applications (*read more*), but testing of these domains is not within the scope of or authorized by the Vulnerability Reward Program.
- **Cross-site scripting vulnerabilities in "sandbox" domains** (*read more*.) We maintain a number of domains that leverage the same-origin policy to safely isolate certain types of untrusted content; the most prominent example of this is "*.googleusercontent.com". Unless an impact on sensitive user data can be demonstrated, we do not consider the ability to execute JavaScript in that domain to be a bug.

malware detection tools, but we do not consider the ability to embed JavaScript within your own blog to be a security bug.

- **URL redirection** (*read more*.) We recognize that the address bar is the only reliable security indicator in modern browsers; consequently, we hold that the usability and security benefits of a small number of well-designed and closely monitored redirectors outweigh their true risks.
- **Legitimate content proxying and framing.** We expect our services to unambiguously label third-party content and to perform a number of abuse-detection checks, but as with redirectors, we think that the value of products such as Google Translate outweighs the risk.
- **Bugs requiring exceedingly unlikely user interaction.** For example, a cross-site scripting flaw that requires the victim to manually type in an XSS payload into Google Maps and then double-click an error message may realistically not meet the bar.
- **Logout cross-site request forgery** (*read more*.) For better or worse, the design of HTTP cookies means that no single website can prevent its users from being logged out; consequently, application-specific ways of achieving this goal will likely not qualify. You may be interested in personal blog posts from Chris Evans and Michal Zalewski for more background.
- **Flaws affecting the users of out-of-date browsers and plugins.** The security model of the web is constantly being fine-tuned. The panel typically does not reward reports that describe issues that affect only the users of outdated or unpatched browsers.
- **Presence of banner or version information.** Version information does not, by itself, expose the service to attacks - so we do not consider this to be a bug. That said, if you find outdated software and have good reasons to suspect that it poses a well-defined security risk, please let us know.
- **Email spoofing on Gmail and Google Groups.** We are aware of the risk presented by spoofed messages and are taking steps to ensure that the Gmail filter can effectively deal with such attacks.
- **User enumeration.** Reports outlining user enumeration are not within scope unless you can demonstrate that we don't have any rate limits in place to protect our users.
- **Bypassing the limit of accounts that can be verified with a given SMS number.** We often receive reports about users being able to bypass our SMS limit for verifying accounts. There are actually two different quotas per number for account verification, one via 'SMS' and a different one via 'Call Me'.

Monetary rewards aside, vulnerability reporters who work with us to resolve security bugs in our products will be credited on the Hall of Fame. If we file an internal security bug, we will acknowledge your contribution on that page.

Google Bug Hunters

New! Vulnerabilities in the Google Cloud Platform are also eligible for additional rewards under the GCP VRP Prize. The total prize money is $313,337 including a top prize of $133,337. See our announcement and the official rules for details and nominate your vulnerability write-ups for the prize here.

Rewards for qualifying bugs range from $100 to $31,337. The following table outlines the usual rewards chosen for the most common classes of bugs. To read more about our approach to vulnerability rewards you can read our article here

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	No integr acquis and o sandb or lo prio applica [3
Vulnerabilities giving direct access to Google servers					
Remote code execution	"Command injection, deserialization bugs, sandbox escapes"	$31,337	$31,337	$31,337	$1,337 - $5,000
Unrestricted file system or database access	"Unsandboxed XXE, SQL injection"	$13,337	$13,337	$13,337	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls	"Direct object reference, remote user impersonation"	$13,337	$7,500	$5,000	$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: "Cross-site scripting" Mobile / Hardware:	$7,500	$5,000	$3,133.7	$100

Other valid security vulnerabilities	Web: “CSRF, Clickjacking” Mobile / Hardware: “Information leak, privilege escalation”	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

“[1] For example, for web properties this includes some vulnerabilities in Google Accounts (https://accounts.google.com).”

“[2] This category includes products such as Google Search (https://www.google.com and https://encrypted.google.com), Google Wallet (https://wallet.google.com), Google Mail (https://mail.google.com), Google Code Hosting (https://code.google.com), Chromium Bug Tracker (https://bugs.chromium.org), Chrome Web Store (https://chrome.google.com), Google App Engine (https://appengine.google.com), Google Admin (https://admin.google.com), Google Developers Console (https://console.developers.google.com), and Google Play (https://play.google.com).”

“[3] Note that acquisitions qualify for a reward only after the initial six-month blackout period has elapsed.”

Reward amounts for abuse-related methodologies

New! Rewards for abuse-related methodologies are based on a different scale and range from USD $100 to $13,337. The reward amount for these abuse-related bugs depends on the potential probability and impact of the submitted technique.

		Impact [1]		
		High	**Medium**	**Low**
Probability [2]	**High**	Up to $13,337	$3,133.7 to $5,000	$1,337
	Medium	$3,133.7 to $5,000	$1,337	$100 to $500
	Low	$1,337	$100 to $500	HoF Credit

“[1] The impact assessment is based on the attack’s potential for causing privacy violations, financial loss, and other user harm, as well as the user-base reached.”

discovered by an attacker."

The final amount is always chosen at the discretion of the reward panel. In particular, we may decide to pay higher rewards for unusually clever or severe vulnerabilities; decide to pay lower rewards for vulnerabilities that require unusual user interaction; decide that a single report actually constitutes multiple bugs; or that multiple reports are so closely related that they only warrant a single reward.

We understand that some of you are not interested in money. We offer the option to donate your reward to an established charity. If you do so, we will double your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Investigating and reporting bugs

When investigating a vulnerability, please, only ever target your own accounts. Never attempt to access anyone else's data and do not engage in any activity that would be disruptive or damaging to your fellow users or to Google.

New! Visit our Bug Hunter University articles to learn more about sending good vulnerability reports.

If you have found a vulnerability, please contact us at goo.gl/vulnz. **Please be succinct**: the contact form is attended by security engineers and a short proof-of-concept link is more valuable than a video explaining the consequences of an XSS bug. If necessary, you can use this PGP key.

Note that we are only able to answer to technical vulnerability reports. Non-security bugs and queries about problems with your account should be instead directed to Google Help Centers.

Frequently asked questions

Q: What if I found a vulnerability, but I don't know how to exploit it?

A: We expect that vulnerability reports sent to us have a valid attack scenario to qualify for a reward, and we consider this to be a critical element of vulnerability research. Reward amounts are

Q: How do I demonstrate the severity of the bug if I'm not supposed to snoop around?

A: Please submit your report as soon as you have discovered a potential security issue. The panel will consider the maximum impact and will choose the reward accordingly. We routinely pay higher rewards for otherwise well-written and useful submissions where the reporter didn't notice or couldn't fully analyze the impact of a particular flaw.

Q: I found an outdated software (e.g. Apache or Wordpress). Does this qualify for a reward?

A: Please perform due diligence: confirm that the discovered software had any noteworthy vulnerabilities, and explain why you suspect that these features may be exposed and may pose a risk in our specific use. Reports that do not include this information will typically not qualify.

Q: Who determines whether my report is eligible for a reward?

A: The reward panel consists of members of the Google Security Team. At the time of this update (January 2021), the current members are: Anna Hupa, Daniel Stelter-Gliese, Gábor Molnár, Jenna Kallaher, John Schwartz, Krzysztof Kotowicz, Marc Henson, Mark Wodrich, Paul Dev, Martin Straka, Eduardo Vela Nava, and Michael Jezierny.

Q: What happens if I disclose the bug publicly before you had a chance to fix it?

A: Please read our stance on coordinated disclosure. In essence, our pledge to you is to respond promptly and fix bugs in a sensible timeframe - and in exchange, we ask for a reasonable advance notice. Reports that go against this principle will usually not qualify, but we will evaluate them on a case-by-case basis.

Q: My report has not been resolved within the first week of submission. Why hasn't it been resolved yet?

A: Reports that deal with potential abuse-related vulnerabilities may take longer to assess, because reviewing our current defense mechanisms requires investigating how a real life attack would take

Q: I wish to report an issue through a vulnerability broker. Will my report still qualify for a reward?

A: We believe that it is against the spirit of the program to privately disclose the flaw to third parties for purposes other than actually fixing the bug. Consequently, such reports will typically not qualify.

Q: What if somebody else also found the same bug?

A: First in, best dressed. You will qualify for a reward only if you were the first person to alert us to a previously unknown flaw.

Q: My employer / boyfriend / dog frowns upon my security research. Can I report a problem privately?

A: Sure. If you are selected as a recipient of a reward, and if you accept, we will need your contact details to process the payment. You can still request not to be listed on our public credits page.

Q: What is bughunter.withgoogle.com?

A: The dashboard for the participants in Google's VRP program. It dynamically creates the hall of fame, i.e., the 0x0A and honorable mentions lists.

Q: Do I need a profile on bughunter.withgoogle.com to participate in the VRP?

A: No. You can participate in the VRP under the same rules without the need of a profile. However, if you want your name to be listed in the 0x0A or the honorable mentions lists, you need to create a profile.

Q: Is the profile data publicly available?

A: Yes. The profile holds the data that is currently already available now on our hall of fame, i.e., on the 0x0A and honorable mentions lists. You can always leave these fields blank.

A: The hall of fame is sorted based on the volume of valid bug submissions, the ratio of valid vs. invalid submissions, and the severity of those submissions.

Q: My account was disabled after doing some tests. How can I get my account restored?

A: We recommend that you create an account dedicated only to testing before beginning any tests on our products, since we cannot guarantee that you will get access back to your account if it is disabled due to your testing activities. If you accidentally used a non-test account or you suspect your personal account was disabled due to your testing, you can request to have your account restored by Signing in to your Google Account and selecting Try to Restore.

Legal points

We are unable to issue rewards to individuals who are on sanctions lists, or who are in countries (e.g. Cuba, Iran, North Korea, Sudan and Syria) on sanctions lists. You are responsible for any tax implications depending on your country of residency and citizenship. There may be additional restrictions on your ability to enter depending upon your local law.

This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time and the decision as to whether or not to pay a reward has to be entirely at our discretion.

Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own.